IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Paul Gassoway
Serial No.:	10/849,318
Filing Date:	May 19, 2004
Group Art Unit:	2436
Examiner:	Oscar A. Louie
Confirmation No.	5789
Title:	**Method and System for Computer Security**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicant respectfully requests reconsideration of the application in light of the remarks set forth below.

REMARKS

Applicant received a Final Office Action dated March 19, 2009 ("Office Action") to which Applicant responded with a response dated May 18, 2009 ("Previous Response"). Applicant received an Advisory Action dated June 3, 2009 ("Advisory Action"). At the time of the Advisory Action, Claims 1-24 were pending, of which, all claims were rejected. Applicant seeks review of the rejections of Claims 1-24.

Claim Objections

The Examiner continues to object to the language "being operable to" Claim 19. However, elements following the term "operable to" in a particular claim element constitute operations that the claim element is capable of performing. Operations that a claim element is capable of performing are limitations because the element is thus distinguished from the prior art that is not capable of performing the operations. Additionally, "operable to" is a commonly used term in patent application claims and is present in claims of numerous patents issued by the United States Patent and Trademark Office. An informal search of the USPTO's website (performed May 13, 2009) returned well over 150,000 issued patents with claims reciting the phrases "operable to" or "being operable to." Therefore, Applicant respectfully requests that this objection be withdrawn.

Rejections under 35 U.S.C. § 103

The Examiner continues to reject Claims 1-5, 7-11, 13-17, and 19-23 under 35 U.S.C. § 103(a) as being unpatentable over *Vaidya* in view of *Nakae*. Claim 1 recites:

> A method for maintaining security of a computer system, comprising:
> determining an initial system certainty value for the computer system;
> providing access to a database of signatures, each signature including a signature certainty value;
> receiving data;
> comparing the received data with the database of signatures;
> increasing the system certainty value if the received data does not match a signature in the database;
> decreasing the system certainty value if the received data matches a signature in the database; and
> filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data.

Applicant respectfully contends that the proposed *Vaidya-Nakae* combination fails to disclose, teach, or suggest every limitation of Claim 1. The Office Action admits that *Vaidya* fails to explicitly disclose the limitations "determining an initial system certainty value for the computer system," "increasing the system certainty value if the received data does not match a signature in the database," and "decreasing the system certainty value if the received data matches a signature in the database." *Office Action*, pgs. 5-6. Instead, the Office Action relies on *Nakae* as disclosing or suggesting these limitations. *Office Action*, pg. 6.

Nakae discloses an attack defending system, including a firewall unit and a decoy device. *Nakae*, ¶¶ 0018-0022. After receiving a data packet, the firewall unit "obtains a corresponding confidence level." *Nakae*, ¶ 0169. This confidence level is compared "with a predetermined threshold value and, depending on its comparison result," the received packet is either forwarded to the internal network or to a decoy device. *Nakae*, ¶ 0169. However, the confidence levels of *Nakae* correspond to the IP address of the received data packet. As such, there are "a set of combinations" of different confidence levels for corresponding IP addresses. Applicant respectfully contends that these multiple confidence levels for the multiple sources of received data fail to teach, disclose, or suggest determining an initial system certainty value for the computer system.

Additionally, the Office Action relies on paragraph 176, lines 3-4 of *Nakae* as disclosing "increasing the system certainty value" and paragraph 239, lines 1-7 of *Nakae* as disclosing "decreasing the system certainty value if the received data matches a signature in the database." *Office Action*, pg. 6. Applicant respectfully contends that, regardless of whether or not the confidence levels of *Nakae* disclose a system certainty value, the Office Action's reliance on the two cited portions of *Nakae* is still misplaced.

First, when a packet is received by firewall 5, the confidence management section 502 (which is part of firewall 5 - *see* ¶ 0168) "obtains a confidence level corresponding to the IP address" of the packet. *Nakae*, ¶ 0174. If no match is found for the IP address, a default initial value is output as the confidence level for that packet. *Id.* at ¶ 0175. After a confidence level is output, the confidence management section 502 increases the relevant confidence value. *Id.* at ¶ 0176. Therefore, according to *Nakae*, the confidence level of a given IP address is increased whenever a packet is received, regardless of whether there is a matching IP address stored in confidence management section 502. As such, Applicant respectfully contends that *Nakae* fails to disclose, teach, or suggest increasing the system certainty value if the received data does not match a signature in the database and decreasing the system certainty value if the received data does match a signature.

Second, in certain instances, the firewall may guide a received IP packet to the decoy unit to determine if there is an attack. If the decoy device detects an attack, it sends an alert and "the confidence level of the source IP address included in the alert is decreased." *Id.* at ¶ 0239. The decoy device detects an attack is occurring based on whether a rule associated with a predetermined attack category is violated. *Id.* at ¶ 0024. However, there is no teaching, disclosure, or suggestion that this determination is based on signatures. As such, applicant respectfully contends that this fails to disclose or suggest decreasing the system certainty value if the received data matches a signature.

The Office Action states that *Nakae* "makes a correlation between increasing/decreasing the confidence level in association with attacks based on information." *Office Action*, pg. 11. Applicant does not necessarily agree. Claim 1 requires increasing the system certainty value if the received data does not match a signature in the database and decreasing the system certainty value if the received data matches a signature. As shown above, the system in *Nakae* increases a confidence level for individual IP addresses whenever a packet is received—regardless of whether the data matches or does not match a signature. Additionally, the system of *Nakae* decreases a confidence level for individual IP addresses whenever an attack is detected, and there is no disclosure or suggestion that this occurs because data either matches or does not match a signature. For at least these reasons, Applicant respectfully contends that *Nakae* fails to disclose, teach, or suggest the limitations "determining an initial system certainty value for the computer system," "increasing the system certainty value if the received data does not match a signature in the database," and "decreasing the system certainty value if the received data matches a signature in the database." Accordingly, Applicant respectfully requests reconsideration and allowance of Claim 1. For substantially similar reasons, Applicant respectfully requests reconsideration and allowance of Claims 2-5, 7-11, 13-17, and 19-23.

The Examiner continues to reject dependent Claims 6, 12, 18, and 24 under 35 U.S.C. § 103(a) as being unpatentable over *Vaidya* in view of *Nakae* and in further view of *Moran*. As discussed above, the proposed *Vaidya-Nakae* combination fails to teach all of the elements of independent Claims 1, 7, 13, and 19. *Moran* fails to overcome these deficiencies. Therefore, Applicant respectfully requests reconsideration and allowance of Claims 6, 12, 18, and 24 for at least the same reasons as discussed above with regard to their respective base claims.

Conclusion

As the rejections of Claims 1-24 contain clear legal and factual deficiencies, Applicant respectfully requests a finding of allowance of Claims 1-24. If the PTO determines that an interview is appropriate, Applicant would appreciate the opportunity to participate in such an interview. To the extent necessary, the Commissioner is hereby authorized to charge any required fees or credit any overpayments to Deposit Account No. **02-0384** of **Baker Botts L.L.P.**

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicant

Luke K. Pedersen
Reg. No. 45,003
Phone: (214) 953-6655

Date: 6-16-09

CORRESPONDENCE ADDRESS:

Customer Number: **05073**